International Journal of Advanced Research Methodology in Engineering & Technology,
Special Issue, March 2017, ISBN 978-1-63535-324-2

QUALITY AND QUANTITY SECURITY ANALYSIS FOR GHOST BASED WIRELESS NETWORKS

Manju Bhagavathy K (*Student*)
Computer Science and Engineering
Sri Ramanujar Engineering College
Chennai, India
manju_be06@yahoo.co.in

Vinod D (*HOD & Associate Professor*)
Information Technology
Sri Ramanujar Engineering College
Chennai, India
dvinopaul@gmail.com

***Abstract* — In Real world, wireless network is prone to Ghost based attack due to mobility of nodes and they are called as moving nodes. Due to its mobility nature, packet loss may occur during the transmission this will leads to data loss or partition of network. In this paper we are proposing a fine grained approach for network adjustment using Localizability aided Localization algorithm to provide information about the localized and non localized nodes in a network. In the proposed approach GPSR protocol a novel routing protocol for wireless datagram networks that uses the positions of routers and a packet's destination in order to make packet forwarding decisions. All the simulation done through the NS-2 module and the results show that Localizability aided Localization algorithm effectively guides the adjustment.**

Keywords — Localization; Localizability; Routing, GPSR; Greedy Forwarding; Perimeter Forwarding;

I. INTRODUCTION

The main objective of the Internet of Things is to integrate and unify of all communications systems that surround us. For example, mobility management in hospitals is required for the clinical devices to be connected through wireless technologies; this allows patients to move freely, continuous monitoring through portable/wearable sensors, and also to extend the coverage within all the hospital, and finally a higher fault tolerance since the mobility management allows the connection to adapt dynamically to different access points. Security is also an inherent requirement for the mobility management, and this enables us to redirect traffic to a new address and claim the identity of a node. Mobility also opens a high number of vulnerabilities for the man in the middle attacks, to identity supplantation, and for data integrity. In order to avoid these vulnerabilities, we require the authentication and also other security mechanism has to be implemented for confidentiality purpose and also to avoid data loss. Theoretical analysis proved that a tuned network is localizable and suitable for localization. The main contributions of this study is to make aware of node localizability, adjustments made by LAL are purposefully selected, avoiding meaningless ranging and communication costs.

II. EXISTING SYSTEM

A three-phase algorithm was proposed by an existing system for analyzing the network flow variations and also to detect and localize the attacker. Number of bogus messages is transmitted by the attacker to lure the receiving victim node to do the superfluous security-related computations, leading to battery depletion. Three phase attack model includes:
(a) Pre-attack phase the attacker learns about the network by surreptitiously eavesdropping the messages
(b) Attack phase in which the attacker leverages the learned information in order to execute the ghost attack; and
(c) Post attack/depletion phase in which, once the energy of nodes are depleted, the attacker executes several other attacks such as replay attack or confidentiality attack.
To further validate the effectiveness of ghost attack, physical experiments were conducted on ZigBee nodes and interestingly, our results show that the lifetime of nodes are significantly impacted with this attack. The existing system does not concentrate much on security they focused only on the energy depletion of the victim nodes.

III. PROPOSED SYSTEM

We put forward a fine-grained approach which is called localizability-aided localization (LAL). This approach basically consists of three phases which include Node localizability checking, Network modification and Structure study. Localizability-aided localization generates a single round adjustment, after which some popular localization methods can be successfully carried out .As our goal in the proposed system is to increase the quality of service, Reliable packet transfer, to detect and avoid DOS and also to increase network life time.

IV. SYSTEM IMPLEMENTATION

In the proposed system localization nodes and non-localization nodes are identified. It contains beacons in the root and the nodes whose position information is already known are placed into a tree like structure. The unlocalized nodes positions are identified using these nodes. By using

GPSR (Greedy Perimeter Stateless Routing) all data packets are forwarded to an adjacent neighbor who is geographically positioned closer to the intended destination. The mechanism followed here is known as greedy forwarding. The forwarding process is done on a packet to packet basis.

This mechanism will lead to failure in situations where the distance between the forwarding node's adjacent neighbors and destination is greater than forwarding node and final destination distance hence we introduced the perimeter mode forwarding. At the same time the data packet is marked as being in perimeter mode along with the location where greedy forwarding gets failed. These perimeter mode packets are forwarded using planar graph traversal. The node will try to make use of the right hand rule to send those packets to nodes while in perimeter mode forwarding. Such nodes are situated counterclockwise to the line joining that forwarding node and the destination. Our goal in the proposed system is to increase the quality of service, Reliable packet transfer, to detect and avoid DOS and also to increase network life time.

V. LAL IMPLEMENTATION

Localizability aided Localization implementation has 3 steps which includes

A. *Step 1 - Localizability testing*

The Node Localizability testing will be done primarily in LAL, which recognizes both localizable and non localizable nodes in a network for further adjustment. This is done since a network may not be prepared for the localization as it might have been deployed in an application field due to environmental factors that are unpredictable in design phase. The best solution is to use the distance graph and to identify all the nodes that are localizable and also to achieve an excellent performance when used practically.

B. *Step 2 - Structure analysis*

The two connected components of a decomposed distance graph will be ordered in a tree like structure. In this tree structure the nodes that contain beacons will be the root. This is done to maintain fine grained manipulation. Adjustments are performed by the side of tree edges from the root to leaves. The root nodes are the nodes whose position is known globally.

C. *Step 3 - Distinctive adjustment*

Location information is the main attribute to detect boundary, routing information and coverage control of network. With the known information of global location of few nodes like becan nodes or anchors the nodes whose position are unknown are identified. The localizability aided localization (LAL) deal with nodes differently according to their localizability and places in the component tree. Through vertex intensification, localizability-aided localization alters all the non-localizable nodes in a single round. The networks tuned by LAL are localizable and can be localized by localization approaches.

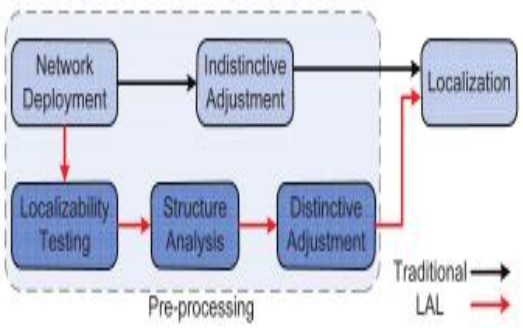

Fig. 1. Localizability aided localization architecture.

VI. GREEDY PERIMETER STATELESS ROUTING

Greedy Perimeter Stateless Routing (GPSR) supports two mechanisms for forwarding data packets. They are Greedy forwarding and Perimeter forwarding

A. *Greedy Forwarding*

In the Greedy forwarding mechanism, all data packets are forwarded to a nearby neighbor that is geographically positioned nearer to the intended destination. This mechanism is called as greedy forwarding. The forwarding will be completed on a packet to packet basis. Hence, least state information is required to be retained by all nodes. It makes protocol mainly fit for the resource starved devices. However, this mechanism is vulnerable to malfunction in situations.

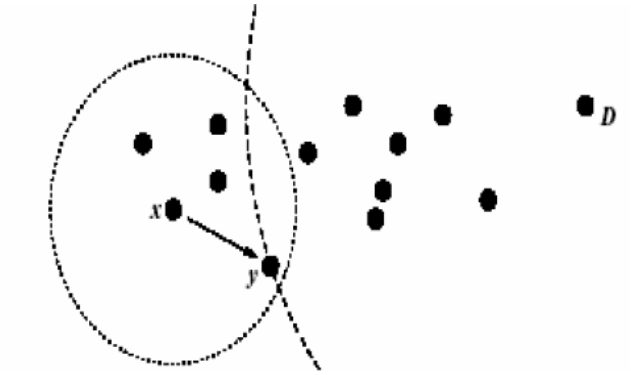

Fig. 2. Greedy Forwarding

B. *Perimeter Forwarding*

In order to surmount routing problems in various scenarios, Greedy Perimeter Stateless Routing will engage perimeter forwarding mode. In perimeter mode, the data packed is marked together with the location where the previous Greedy forwarding has not been passed. This perimeter mode data packet is forwarded using simple planar graph traversal. The node will try to make use of the right

hand rule to send those packets to nodes while in perimeter. Such nodes are situated counterclockwise to the line joining that forwarding node and the destination. When forwarding perimeter mode packets, each node evaluates from the point of its current distance to the destination where greedy forwarding has failed. If the current distance is less, packet will be routed through the greedy forwarding from that point onward repeatedly.

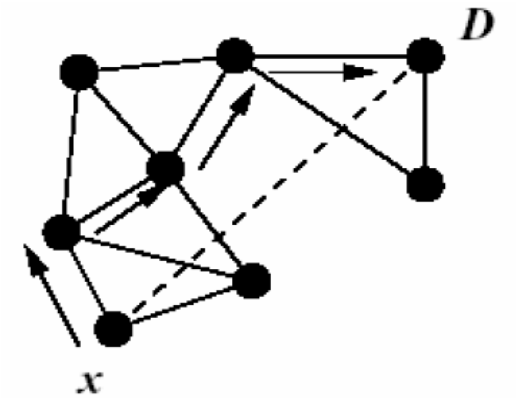

Fig. 3. Perimeter Forwarding

VII. The Network Model

The small circles with number are named as nodes. The source node is named as number node zero and the destinations are marked in Fig.4 below. The source need to send the message to various destinations through the optimal path foundation using random wave point generator which helps to identify the location of becan nodes and localized nodes in the component tree and it also helps to identify non localized node to involve in the path detecting and preventing denial of service attack.

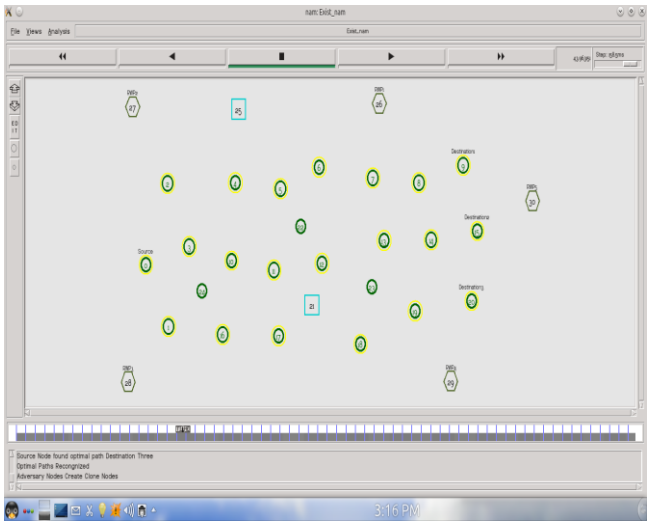

Fig. 4. Working of Node

VIII. Results and Discussions

The comparison of result is analyzed through graph using the network simulator. During transmission the delay of packet is compared between existing and proposed system. In the proposed system there is a drastic fall of delay is represented with brown colour.

The x axis indicates the time limit and the y axis indicate the delay ratio. The comparison is shown in Fig.5 by using two colour. The existing system has been indicated with brown colour and the proposed system indicated with green colour. Since we used the Greedy Perimeter Stateless Routing the delay has been significantly reduced.

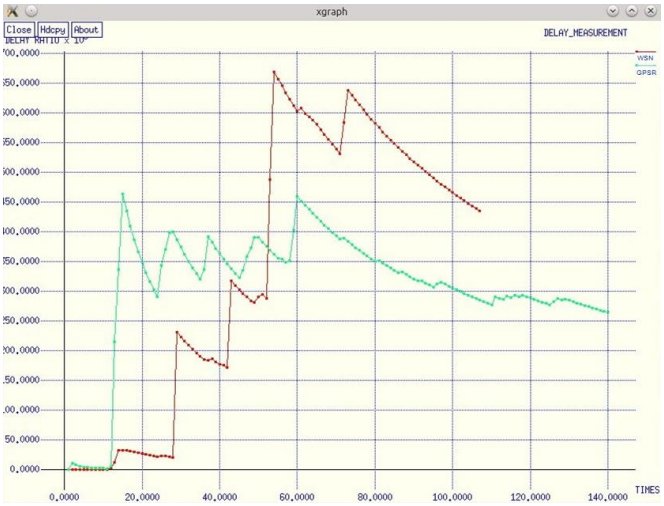

Fig. 5. Delay Measurement

The throughput of proposed system is high when compared with the existing system. The comparison of result has been shown in Fig.6. The green colour indicate the throughput in proposed system.

Fig. 6. Comparison of through-put

In the proposed system the loss ratio is low when compared with the existing system. The result in Fig 7 is shown by indicating in two different colours. The packet delivered is low in existing system when compared with proposed system. The x axis denotes the packet delivery ratio time and y axes indicate the packet loss.

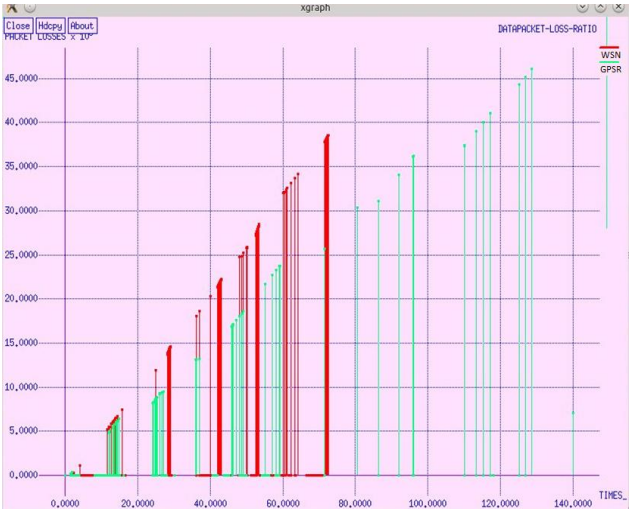

Fig. 7. Loss Ratio during Transmission

IX. Conclusion

In this paper an efficient routing scheme is proposed with location based (GPSR) protocol to improve the utilization of node localization. The modification of localization in non localizable network, and proposed the new technique of the localizability aided localization approach is named as LAL. It has the result in node localizability with indistinctive consideration. The LAL authenticate its potency through working experiments and simulations are evaluated. However there are still more work to be done, so that the best route is optimized and message is delivered from sender to receiver with less number of packet drop. In our simulation experiments, we simulated the normal routing load, packet delivery ratio etc with reliable packet transfer, Quality of service improved, increasing in network lifetime and detecting and avoiding denial of service attack.

References

[1] Xianghui Cao, Member, , Devu Manikantan Shila, Yu Cheng, Senior Member, Zequ Yang, Yang Zhou, and Jiming Chen, Senior Member, "Ghost-in-ZigBee: Energy Depletion Attack on ZigBee based Wireless Networks", IEEE Internet Things

[2] Darshana 1, Sandeep Mann 2, 1 Department of Information Technology, 2 Department of Computer Science 1Banasthali University, Jaipur Campus, Rajasthan, India, 2 Assistant Professor, Government College, Gurgaon, Haryana, India. khd2509@gmail.com, sandeep.mann23@gmail.com, "Greedy Perimeter Stateless Routing In Vehicular Ad- Hoc Networks"

[3] J. A. Stankovic, "Research directions for the internet of things," IEEE Internet Things J., vol. 1, no. 1, pp. 3–9, 2014.

[4] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," IEEE Internet Things J., vol. 1, no. 4, pp. 289–299, 2014.

[5] Y. Liu, C. Yuen, X. Cao, N. Ul Hassan, and J. Chen, "Design of a scalable hybrid MAC protocol for heterogeneous M2M networks," IEEE Internet Things J., vol. 1, no. 1, pp. 99–111, 2014

[6] Y. Zhang, S. He, and J. Chen, "Data gathering optimization by dynamic sensing and routing in rechargeable sensor networks," IEEE/ACM Trans. Netw., dOI:10.1109/TNET.2015.2425146, to appear.

[7] K. Chebrolu and A. Dhekne, "Esense: energy sensing-based cross-technology communication," IEEE Trans. Mobile Comput., vol. 12, no. 11, pp. 2303–2316, 2013.

[8] Y. Xiao, H. Chen, B. Sun, R. Wang, and S. Sethi, "MAC security and security overhead analysis in the IEEE 802.15.4 wireless sensor networks," EURASIP J. Wirel. Comm., vol. 2006, 2006.

[9] K. Zhang, X. Liang, R. Lu, and X. S. Shen, "Sybil attacks and their defenses in the internet of things," IEEE Internet Things J., vol. 1, no. 5, pp. 372–383, 2014.

[10] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal dos attack scheduling in wireless networked control system," IEEE Trans. Control Syst. Technol., dOI:10.1109/TCST.2015.2462741, to appear.

[11] IEEE Computer Society, "Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)," IEEE Sandard 802.15.4, 2006.

[12] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in Proc. ACM workshop on Wireless security, 2004, pp. 32–42.

[13] J. Zheng, M. J. Lee, and M. Anshel, "Toward secure low rate wireless personal area networks," IEEE Trans. Mobile Comput., vol. 5, no. 10, pp. 1361–1373, 2006.

[14] M. Doomun, K. Soyjaudah, and D. Bundhoo, "Energy consumption and computational analysis of Rijndael-AES," in Proc. IEEE/IFIP Int. Conf. in Central Asia on Internet, 2007, pp. 1–6.

[15] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," IEEE Trans. Veh. Technol., vol. 58, no. 1, pp. 367–380, 2009.

[16] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, "The sleep deprivation attack in sensor networks: Analysis and methods of defense," Int. J. Distrib. Sens. N., vol. 2, no. 3, pp. 267–287, 2006.

[17] T. Bhattasali, R. Chaki, and S. Sanyal, "Sleep deprivation attack detection in wireless sensor network," International Journal of Computer Applications, vol. 40, no. 15, pp. 19–25, 2012.

[18] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 8, pp. 1119–1133, 2010.

[19] E. Y. Vasserman and N. Hopper, "Vampire attacks: draining life from wireless ad hoc sensor networks," IEEE Trans. Mobile Comput., vol. 12, no. 2, pp. 318–332, 2013.